A Simplified Algorithm for Correcting Both Errors and Erasures of R-S Codes

I. S. Reed
University of Southern California

T. K. Truong
TDA Engineering Office

Using the finite field transform and continued fractions, a simplified algorithm for decoding Reed-Solomon codes is developed to correct erasures caused by other codes as well as errors over the finite field $GF(q^m)$, where q is a prime and m is an integer. Such an R-S decoder can be faster and simpler than a decoder that uses more conventional methods.

I. Introduction

Fast real-valued transforms over the group $(Z_2)^m$ were used first by Green (Ref. 1) to decode the (32, 6) Reed-Muller code (Ref. 2) used by the Jet Propulsion Laboratory (JPL) in Mariner and Viking space probes. Gore (Ref. 3) extended Mandelbaum's methods (Ref. 4) for decoding R-S codes (Ref. 5). He proposed to decode R-S codes with a finite field transform over $GF(2^m)$, where m is an integer. Michelson (Ref. 6) implemented Mandelbaum's algorithm and showed that the decoder, using the transform over $GF(2^m)$, requires substantially fewer multiplications than the standard decoder (Ref. 7). Recently, it was shown (Ref. 8) that R-S codes can be decoded efficiently with a combination of the fast transform method and continued fractions.

For a space communication link, it was shown in (Ref. 9) that an R-S code that is concatenated with a Viterbi-decoded convolutional code can be used to reduce the signal-to-noise ratio required to meet a specified bit error rate. Such a concatenated R-S code is implemented presently on the Voyager spacecraft.

In such a concatenated code, the inner convolutional decoder is sometimes able to find only two or more equally probable R-S symbols. Then it is possible to declare an erasure of the R-S symbol, i.e., mark the location of a possible error. The outer R-S code can take advantage of the knowledge of these erasure locations if erasures are reported to the R-S decoder by the Viterbi decoder. Erasures are not reported by the MCD as presently implemented in the DSN.

In this article, a simplified decoding algorithm is developed to correct erasures and errors of R-S codes using both a finite transform and continued fractions. This decoding algorithm is based on the algorithm originally invented by Forney (Refs. 10 and 11). An important advantage of the present decoding technique over previous methods is that a Chien-type search (Refs. 7 and 11) for the roots of the error locator polynomial is completely avoided.

II. On the Decoding of Erasures and Errors

Let n be the block length of an R-S code in $GF(q^m)$. Also let d be the minimum distance of the code where $d = P - 1$. Then $n = P + I$, where P is the number of parity symbols and I is the number of information symbols.

Define the following five different vectors:

$(c_0, c_1, \cdots, c_{n-1})$ = **c**, code vector

$(r_0, r_1, \cdots, r_{n-1})$ = **r**, received vector

$(u_0, u_1, \cdots, u_{n-1})$ = **u**, erasure vector

$(e_0, e_1, \cdots, e_{n-1})$ = **e**, error vector

$(\tilde{u}_0, \tilde{u}_1, \cdots, \tilde{u}_{n-1})$ = $\tilde{\mathbf{u}}$, new erasure vector

These vectors are related by $\tilde{\mathbf{u}} = \mathbf{e} + \mathbf{u}$ and $\mathbf{r} = \mathbf{c} + \mathbf{u} + \mathbf{e}$.

Suppose that t errors and s erasures occur in the received vector **r** and that $s + 2t \leqslant d - 1$. The syndromes are given by

$$S_k = r(\alpha^k) = \sum_{i=0}^{n-1} r_i \alpha^{ki}$$

$$= \sum_{i=0}^{n-1} c_i \alpha^{ki} + \sum_{i=0}^{n-1} u_i \alpha^{ki} + \sum_{i=0}^{n-1} e_i \alpha^{ki} \qquad \text{for } 1 \leqslant k \leqslant d - 1$$

but

$$\sum_{i=0}^{n-1} c_i \alpha^{ki} = 0 \qquad \text{for } 1 \leqslant k \leqslant d - 1$$

Thus

$$S_k = \sum_{i=0}^{n-1} u_i \alpha^{ki} + \sum_{i=0}^{n-1} e_i \alpha^{ki}$$

$$= \sum_{j=1}^{s} W_j Z_j^k + \sum_{j=1}^{t} Y_j X_j^k \equiv E_k \qquad \text{for } 1 \leqslant k \leqslant d - 1 \qquad (1a)$$

In general, let

$$E_k = \sum_{j=1}^{t} Y_j X_j^k + \sum_{j=1}^{s} W_j Z_j^k \qquad \text{for all } k \qquad (1b)$$

where Y_j is the j-th error amplitude, X_j is the j-th error location, W_j is the j-th erasure amplitude, Z_j is the j-th known erasure location, and $E_k = S_k$ is known for $1 \leqslant k \leqslant d - 1$.

Following Forney, let the erasure locator polynomial be defined by

$$\tau(x) = \prod_{j=1}^{s} (x - Z_j) = \sum_{j=0}^{s} (-1)^j \tau_j x^{s-j} \qquad (2)$$

This implies

$$\sum_{j=0}^{s} (-1)^j \tau_j Z_k^{s-j} = 0 \qquad \text{for } k = 1, 2, \cdots, s \qquad (3)$$

where $\tau_0 = 1$ and τ_j's are known functions of $Z_1, Z_2, \cdots, Z_s$ for $1 \leqslant j \leqslant s$. The Forney syndrome (Ref. 10) is defined by

$$T_i = \sum_{j=0}^{s} (-1)^j \tau_j S_{i+s-j} \qquad \text{for } 1 \leqslant i \leqslant d - 1 - s \qquad (4a)$$

From Eqs. (1a) and (3), we know that τ_j for $j = 1, 2, \cdots, s$ and S_k for $k = 1, 2, \cdots, d - 1$ is known. Thus the T_i's for $1 \leqslant i \leqslant d - 1 - s$ are known. In general, let

$$T_i = \sum_{j=0}^{s} (-1)^j \tau_j E_{i+s-j} \qquad \text{for all } i \qquad (4b)$$

where $E_{i+s-j} = S_{i+s-j}$ for $1 \leqslant i + s - j \leqslant d - 1$. Then the Forney syndrome T_i is known for $1 \leqslant i \leqslant d - 1 - s$.

Now if one substitutes Eq. (1b) into Eq. (4b),

$$T_i = \sum_{j=0}^{s} (-1)^j \tau_j E_{i+s-j}$$

$$= \sum_{j=0}^{s} (-1)^j \tau_j \left[\sum_{k=1}^{t} Y_k X_k^{i+s-j} + \sum_{k=1}^{s} W_k Z_k^{i+s-j} \right]$$

$$= \sum_{k=1}^{t} Y_k X_k^i \sum_{j=0}^{s} (-1)^j \tau_j X_k^{s-j}$$

$$+ \sum_{k=1}^{s} W_k Z_k^i \sum_{j=0}^{s} (-1)^j \tau_j Z_k^{s-j}$$

From Eq. (3) one observes

$$\sum_{k=0}^{s} W_k Z_k^i \sum_{j=0}^{s} (-1)^j \tau_j Z_k^{s-j} = 0$$

Thus,

$$T_i = \sum_{k=1}^{t} Y_k X_k^i \sum_{j=0}^{s} (-1)^j \tau_j X_k^{s-j}$$

$$= \sum_{k=1}^{t} D_k X_k^i \qquad \text{for all } i \tag{5}$$

where the quantities

$$D_k = Y_k \sum_{j=0}^{s} (-1)^j \tau_j X_k^{s-j}$$

for $k = 1, 2, \cdots, t$ are not known.

Now let $T(x)$ be a formal power series in the indeterminate x, defined by

$$T(x) = T_1 x^{-1} + T_2 x^{-2} + T_3 x^{-3} + \cdots$$

$$+ T_{d-1-s} x^{-(d-1-s)} + \cdots \tag{6}$$

Then substituting Eq. (5) into Eq. (6), gives

$$T(x) = \sum_{i=1}^{\infty} T_i x^{-i} = \sum_{i=1}^{\infty} \left(\sum_{k=1}^{t} D_k X_k^i \right) x^{-i}$$

$$= \sum_{k=1}^{t} D_k \sum_{i=1}^{\infty} (X_k x^{-1})^i$$

$$= \sum_{k=1}^{t} D_k \frac{X_k x^{-1}}{1 - X_k x^{-1}} = \sum_{k=1}^{t} D_k \frac{X_k}{x - X_k} = \frac{p(x)}{\sigma(x)} \tag{7}$$

where

$$\sigma(x) = \prod_{k=1}^{t} (x - X_k)$$

is the error locator polynomial and $\deg p(x) < \deg \sigma(x)$. Since T_i is known for $i = 1, 2, \cdots, d - 1 - s$, where $t \leqslant d - 1$, then, by Theorem 2 in Ref. 8, the error locator $\sigma(x)$ can be obtained by using continued fractions. The roots of $\sigma(x)$ are the locations of the t errors.

Since the locations of the t errors and the s erasures are now known, we may assume that we have the problem of only s' erasures where $s' = t + s$. That is, the only unknowns are the "erasure" amplitudes $\widetilde{W}_1, \widetilde{W}_2, \cdots, \widetilde{W}_{s'}$, the amplitudes of both the error and erasure vectors. The corresponding known locators are $\widetilde{Z}_1, \widetilde{Z}_2, \cdots, \widetilde{Z}_{s'}$. Only the case of erasures need be considered.

Suppose there are $s' \leqslant d - 1$ erasures. Then $\mathbf{r} = \mathbf{c} + \widetilde{\mathbf{u}}$, where $\widetilde{\mathbf{u}} = \mathbf{u} + \mathbf{e}$ is a new erasure vector in which s' erasures occur where the received vector is $\mathbf{r}$ and $\mathbf{c}$ is the code vector. The syndromes are

$$\widetilde{S}_k = r(\alpha^k) = \sum_{i=0}^{n-1} r_i \alpha^{ki} = \sum_{i=0}^{n-1} c_i \alpha^{ki} + \sum_{i=0}^{n-1} \widetilde{u}_i \alpha^{ik}$$

$$\text{for } k = 1, 2, \cdots, d - 1$$

but

$$\sum_{i=0}^{n-1} c_i \alpha^{ki} = 0 \qquad \text{for } k = 1, 2, \cdots, d - 1$$

Thus

$$\widetilde{S}_k = \sum_{i=0}^{n-1} \widetilde{u}_i \alpha^{ki}$$

$$= \sum_{j=1}^{s'} \tilde{W}_j \tilde{Z}_j^k \equiv U_k \qquad \text{for } k = 1, 2, \cdots, d-1 \qquad (8a)$$

where $\tilde{W}_j$ are the j-th amplitudes of the erasure and error vectors and $\tilde{Z}_j$ are the j-th known locations of the original erasure and error vectors. Note that $\tilde{S}_k$ actually equals S_k in Eq. (1a) for $k = 1, 2, \cdots, d-1$. In general, let

$$U_k = \sum_{j=1}^{s'} \tilde{W}_j \tilde{Z}_j^k \qquad \text{for all } k \qquad (8b)$$

where $U_k = \tilde{S}_k$ for $k = 1, 2, \cdots, d-1$. The erasure polynomial of the original erasure and error vector is given by

$$\tilde{\tau}(x) = \sum_{j=1}^{s'} (x - \tilde{Z}_j) = \sigma(x)\tau(x) = \sum_{k=0}^{s'} (-1)^k \tilde{\tau}_k x^{s'-k}$$

where $\tilde{\tau}_0 = 1$, $s' = t + s$, and $\tau(x)$ and $\sigma(x)$ are given in Eqs. (2) and (7), respectively. Hence

$$\tilde{\tau}(\tilde{Z}_i) = \sum_{k=0}^{s'} (-1)^k \tilde{\tau}_k \tilde{Z}_i^{s'-k} = 0 \qquad \text{for } i = 1, 2, \cdots, s' \qquad (9)$$

Multiplying Eq. (9) by $\tilde{W}_i \tilde{Z}_i^j$,

$$\tilde{W}_i \tilde{Z}_i^{s'} \tilde{Z}_i^j + \sum_{k=1}^{s'} (-1)^k \tilde{\tau}_k \tilde{W}_i \tilde{Z}_i^{s'-k} Z_i^j \qquad (10)$$

Summing Eq. (10) on i for $i = 1, 2, \cdots, s'$, yields

$$\sum_{i=1}^{s'} \tilde{W}_i \tilde{Z}_i^{s+j} + \sum_{i=0}^{s'} \sum_{k=1}^{s'} (-1)^k \tilde{\tau}_k \tilde{W}_i \tilde{Z}_i^{s'+j-k} = 0$$

Thus

$$U_{s+j} + \sum_{k=1}^{s'} (-1)^k \tilde{\tau}_k U_{s+j-k} = 0 \qquad \text{for } j \geqslant 1$$

In general,

$$U_\ell = -\sum_{k=1}^{s'} (-1)^k \tilde{\tau}_k U_{\ell-k} = 0 \qquad \text{for } \ell > d-1 \qquad (11)$$

where $U_1, U_2, \cdots, U_{d-1}$ are known. From Eq. (11) one obtains the rest of the transform of $\tilde{\mathbf{u}}$, i.e., U_ℓ for $0 \leqslant \ell \leqslant n-1$. The vector of amplitudes $\tilde{\mathbf{u}}$ is found by taking the inverse transform over $GF(q^m)$ of U_ℓ for $\ell = 0, 1, 2, \cdots, n-1$. Finally, the original n-tuple code vector can be obtained by subtracting $\tilde{\mathbf{u}}$ from the received vector $\mathbf{r}$.

Let us recapitulate the decoding of R-S codes for both errors and erasures using the transform over $GF(q^m)$ and continued fractions. This algorithm is composed of the following five steps:

(a) Compute the transform over $GF(q^m)$ of the received vector n-tuple, $(r_0, r_1, \cdots, r_{n-1})$, i.e.,

$$S_k = \sum_{i=0}^{n-1} r_i \alpha^{ik} = U_k \qquad k = 0, 1, \cdots, d-1$$

where $r_i \in GF(q^m)$, α is an element of order n, and d is the minimum distance of the R-S code.

(b) Compute τ_j for $j = 0, 1, 2, \cdots, s$ from the erasure locator polynomial

$$\tau(x) = \prod_{j=1}^{s} (x - Z_j) = \sum_{j=0}^{s} (-1)^j \tau_j x^{s-j}$$

where s is the number of erasures in the received vector. The Z_j's for $1 \leqslant j \leqslant s$ are the known erasure locations. Then compute the Forney syndrome T_n for $1 \leqslant n \leqslant d-1-s$ from the equation

$$T_i = \sum_{j=0}^{s} (-1)^j \tau_j E_{i+s-j} \qquad \text{for } 1 \leqslant i \leqslant d-1-s$$

where τ_j for $1 \leqslant j \leqslant s$ and $E_j = S_j$ for $1 \leqslant j \leqslant d-1$ are known.

(c) Use continued fractions to determine the error locator polynomial $\sigma(x)$ from the known T_i's for $1 < i \leqslant d-1-s$.

(d) Compute the erasure and error locator polynomials from the equation

$$\tilde{\tau}(x) = \sigma(x)\tau(x) = \sum_{k=0}^{s+t} (-1)^j \tilde{\tau}_k x^{s+t-j}$$

where $\sigma(x)$ and $\tau(x)$ are the known polynomial. Then

compute the rest of the transform of the erasure and error vector from the equation

$$U_\ell = \sum_{k=1}^{s+t} (-1)^k \tilde{\tau}_k U_{\ell-k} \qquad \text{for } \ell > d-1$$

where $U_\ell = S_\ell$ for $1 \leqslant \ell \leqslant d-1$.

(e) Invert the transform to recover the error and erasure vector, then obtain the corrected code vector.

To illustrate the decoding procedure for correcting errors with erasures, a simple example of an R-S code over $GF(17)$ is now presented.

Example: Let $GF(17)$ be the field of integers, modulo the Fermat prime $F_2 = 2^{2^2} + 1 = 17$. We consider the correction of one error and two erasures in an eighttuple R-S code over $GF(17)$. For this case $n = 8$, $d-1 = P = 4$, $t = 1$, $s = 2$, and $d - 1 = 2t + s$.

Let $\mathbf{c} = (5, 2, 12, 15, 2, 3, 2, 1)$ be transmitted. Assume the erasure vector is $\mathbf{u} = (0, 0, -3, 0, 0, -2, 0, 0)$ and the error vector is $\mathbf{e} = (0, 2, 0, 0, 0, 0, 0, 0)$. Then $\tilde{\mathbf{u}} = \mathbf{u} + \mathbf{e} = (0, 2, -3, 0, 0, -2, 0, 0)$ is a new erasure vector. Hence the received vector is $\mathbf{r} = \mathbf{c} + \mathbf{u} + \mathbf{e} = (5, 4, 9, 15, 2, 1, 2, 1)$.

Now the syndromes S_k for $\mathbf{r}$ are

$$U_k = S_k = r(2^k) = \sum_{i=0}^{7} r_i 2^{ki}$$

$$= 2(2^k)^1 - 3(2^k)^2 - 2(2^k)^5$$

$$\text{for } 1 \leqslant k \leqslant d-1 = 4$$

That is, $U_1 = S_1 = -4$, $U_2 = S_2 = 3$, $U_3 = S_3 = 10$, and $U_4 = S_4 = -3$. The erasure locator polynomial is given by

$$\tau(x) = \prod_{i=1}^{2} (x - Z_i) = (x - 2^2)(x - 2^5) = (x - 4)(x - 32)$$

$$= x^2 - 2x + 9$$

Thus we obtain $\tau_0 = 1$, $\tau_1 = 2$, and $\tau_2 = 9$. Then the Forney syndromes are

$$T_n = \sum_{j=0}^{s} (-1)^j \tau_j S_{n+s-j} = \sum_{j=0}^{2} (-1)^j \tau_j S_{n+2-j}$$

$$= S_{n+2} - 2S_{n+1} + 9S_n \qquad \text{for } 1 \leqslant n \leqslant d-1-s = 2$$

Hence $T_1 = 2$, and $T_2 = 4$. The power series for $T(x)$ is

$$T(x) = T_1 x^{-1} + T_2 x^{-2} + \cdots + T_{d-1-s} x^{-(d-1-s)} + \cdots$$

$$= 2x^{-1} + 4x^{-2} + ?x^{-3} + \cdots = \frac{D(x)}{\sigma(x)}$$

Since $d - 1 - s = 2t = 2$, by Theorem 2 in Ref. 8, $\sigma(x)$ can be determined by the use of continued fractions. Thus, $T(x) = 2/(x - 2)$. Hence $\sigma(x) = x - 2$.

The erasure and error locator polynomial is

$$\tilde{\tau}(x) = \sigma(x)\tau(x) = (x - 2)(x^2 - 2x + 9) = x^3 - 4x^2 + 13x - 1$$

Thus, $\tilde{\tau}_0 = 1$, $\tilde{\tau}_1 = 4$, $\tilde{\tau}_2 = -4$, and $\tilde{\tau}_3 = 1$. The rest of the transform for $\tilde{\mathbf{u}}$ is given by

$$E_k = \tilde{\tau}_1 U_{k-1} - \tilde{\tau}_2 U_{k-2} + \tilde{\tau}_3 U_{k-3}$$

$$= 4U_{k-1} + 4U_{k-2} + 1U_{k-3} \qquad \text{for } k \geqslant 5$$

Thus, $U_5 = -3$, $U_6 = 3$, $U_7 = -3$, and $U_8 = U_0 = -3$. The inverse transform over $GF(17)$ of the U_k for $0 \leqslant k \leqslant 7$ is given by

$$\tilde{u}_i = 8^{-1} \sum_{k=2}^{7} U_k 2^{-ik} = (-2) \sum_{k=0}^{7} U_k 2^{-ik}$$

$$\text{for } i = 0, 1, 2, \cdots, 7$$

Hence, $\tilde{\mathbf{u}} = (0, 2, -3, 0, 0, -2, 0, 0)$. The corrected code vector is thus

$$\mathbf{c} = \mathbf{r} - \tilde{\mathbf{u}} = (5, 4, 9, 15, 2, 1, 2, 1) - (0, 2, -3, 0, 0, -2, 0, 0)$$

$$= (5, 2, 12, 15, 2, 3, 2, 1)$$

Acknowledgement

The authors wish to thank Dr. N. A. Renzetti, Manager of Tracking and Data Acquisition Engineering of the Jet Propulsion Laboratory for his continued support and encouragement of the research which led to this paper. The first author also appreciates the encouragement and support he got from Mr. Glen W. Prestor of the Institute for Defense Analyses to pursue this topic.

References

1. Green, R. R., "Analysis of a Serial Orthogonal Decoder," *Space Programs Summary 37-53*, Vol. III, 1968, pp. 185-187. Jet Propulsion Laboratory, Pasadena, California.
2. Reed, I. S., "A Class of Multiple Error-Correcting Codes and the Decoding Scheme," *IRE Trans.*, PFIT-4, 1954, pp. 38-49.
3. Gore, W. C., *Transmitting Binary Symbols with Reed-Solomon Code*, Johns Hopkins EE Report No. 73-75, April 1973.
4. Mandelbaum, D., "On Decoding Reed-Solomon Codes," *IEEE Trans. on Inform. Theory*, Vol. IT-17, No. 6, November 1971, pp. 707-712.
5. Reed, I. S., and Solomon, G., "Polynomial Codes Over Certain Finite Fields," *J. Soc. Indus. Appl. Math.*, Vol. 8, June 1960, pp. 300-304.
6. Michelson, A., *A New Decoder for the Reed-Solomon Codes Using a Fast Transform Technique*, Systems Engineering Technical Memorandum No. 52, Electronic Systems Group Eastern Division GTE Sylvania, August 1975.
7. Peterson, W. W., *Error-Correcting Codes*, MIT Press, Cambridge, Mass., 1961, pp. 168-169.
8. Reed, I. S., Scholtz, R. A., Truong, T. K., and Welch, L. R., "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions," *IEEE Trans. on Inform. Theory*, Vol. IT-24, No. 1, January 1978, pp. 100-106.
9. Odenwalder, J., et al., *Hybrid Coding Systems Study Final Report*, Linkabit Corp., NASA CR 114, 486, September 1972.
10. Forney, G. D., "On Decoding BCH Codes," *IEEE Trans. on Inform. Theory*, Vol. IT-11, October 1965, pp. 549-557.
11. Berlekamp, E. R., *Algebraic Coding Theory*, McGraw Hill, New York, 1968.